10 loại malware điển hình

Hiện nay, ngày càng có nhiều loại malware mới tinh vi hơn, độc hại hơn xuất hiện. Ai cũng có thể biết đến những tác hại mà malware gây ra, nhưng không phải ai cũng biết đến cách thức hoạt động của chúng. Bài viết này sẽ điểm ra 10 loại malware được cho là nguy hiểm nhất từ trước tới nay.

Dưới đây là một số thuật ngữ được sử dụng trong bài viết:

- *Malware*: Là một phần mềm độc hại được viết ra chuyên để xâm nhập và phá hủy hệ thống máy tính mà người dùng không hề hay biết.
- *Malcode*: Là một mã lập trình độc hại được nhúng vào giai đoạn phát triển của một ứng dụng phần mềm và thường nằm trong payload của malware, dùng để thực thi những hoạt động phá hoại, lấy cắp thông tin trên máy tính.
- *Anti-malware:* Bao gồm những chương trình chống lại malware, giúp bảo vệ, phát hiện và gỡ bỏ malware. Ứng dụng antivirus, anti-spyware và ứng dụng phát hiện malware là những ví dụ của anti-malware.

1. Virus máy tính khét tiếng

Virus máy tính là một malware có thể lây nhiễm nhưng phải dựa vào những phương tiện khác để phát tán. Một loại virus thật sự có thể lan tràn từ những máy tính bị nhiễm tới một máy tính chưa nhiễm bằng cách đính một mã vào file thực thi được truyền qua nhau. Ví dụ, một virus có thể ẩn trong một file PDF được đính vào một email. Hầu hết virus đều gồm có 3 thành phần sau:

- **Replicator:** Khi kích hoạt chương trình chủ thì đồng thời virus cũng được kích hoạt, và ngay lập tức chúng sẽ phát tán malcode.
- **Concealer:** Biện pháp virus sử dụng để lẩn tránh anti-malware.

- **Payload:** Như đã nói, payload này thường là malcode của một virus, được sử dụng để vô hiệu hóa các chức năng của máy tính và phá hủy dữ liệu.

Một số mẫu virus máy tính gần đây gồm W32.Sens.A, W32.Sality.AM, và W32.Dizan.F. Hầu hết những phần mềm chống virus tốt sẽ gỡ bỏ virus dựa trên file dữ liệu virus của mình.

2. Sâu (Worm)

Sâu máy tính tinh vi hơn nhiều so với virus. Chúng có thể tự sao chép mà không cần tới can thiệp của người dùng. Malware sẽ giống sâu hơn virus nếu sử dụng Internet để phát tán. Những thành phần chính của sâu bao gồm:

- **Penetration tool**: Là malcode khai thác những lỗ hổng trên máy tính của nạn nhân để dành quyền truy cập.
- **Installer**: Công cụ thâm nhập giúp sâu máy tính vượt qua hệ thống phòng thủ đầu tiên. Lúc đó, installer sẽ tiếp nhận và chuyển thành phần chính của malcode vào máy tính của nạn nhân.
- **Discovery tool**: Khi đã xâm nhập vào máy, sâu sử dụng cách thức để truy lục những máy tính khác trên mạng, gồm địa chỉ email, danh sách máy chủ và các truy vấn DNS.
- **Scanner**: Sâu sử dụng một công cụ kiểm tra để xác định những máy tính mục tiêu mới trong penetration tool có lỗ hổng để khai thác.
- **Payload**: Malcode tồn tại trên mỗi máy tính của nạn nhân. Những malcode này có thể là bất cứ thứ gì, từ một ứng dụng truy cập từ xa đến một key logger được dùng để đánh cắp tên đăng nhập và mật khẩu của người dùng.

Thật không may loại malware này lại sinh sôi rất nhanh. Khởi đầu với sâu Morris vào năm 1988 và hiện nay là sâu Conficker. Hầu hết sâu máy tính có thể gỡ bỏ bằng chương trình quét malware.

3. Backdoor

Backdoor giống với những chương trình truy cập từ xa mà chúng ta thường sử dụng. Chúng được coi là malware nếu cài đặt mà không có sự cho phép, đây chính xác là những gì mà hacker muốn, theo các phương thức sau:

- Khai thác lỗ hổng trên máy tính mục tiêu.
- Bẫy người dùng cài đặt backdoor thông qua một chương trình khác.

Sau khi được cài đặt, backdoor cho phép tin tặc toàn quyền kiểm soát từ xa những máy tính bị tấn công. Những loại backdoor, như SubSeven, NetBus, Deep Throat, Back Orifice và Bionet, đã được biết đến với phương thức này.

4. Trojan horse

Theo Ed Skoudis và Lenny Zelter, Trojan horse là một chương trình thoạt nhìn có vẻ hữu dụng, an toàn nhưng trong nó lại ẩn chứa nhiều "tính năng" độc hại.

Trojan horse malware chứa đựng nhiều payload phá hoại trong khi cài đặt và chạy chương trình, ngăn cản malware nhận ra malcode. Một số kĩ thuật che giấu bao gồm:

- Đổi tên malware thành những file giống với file bình thường trên hệ thống.
- Làm lỗi phần mềm diệt virus được cài trên máy tính, nhằm ngăn nó phản hồi khi malware bị phát hiện.
- Sử dụng nhiều loại code khác nhau để thay đổi đăng ký của malware nhanh hơn những phần mềm bảo mật.

Vundo là loại Trojan horse điển hình. Nó tạo ra nhiều quảng cáo popup để quấy rối những chương trình chống spyware, làm suy giảm khả năng thực thi của hệ thống và cản trở trình duyệt web. Nếu dính con trojan này bạn sẽ phải cài phần mềm diệt virus trên LiveCD để phát hiện và gỡ bỏ nó.

5. Adware/spyware

Adware là phần mềm tạo ra popup quảng cáo mà không có sự cho phép của người dùng. Adware thường được cài đặt bởi một thành phần của phần mềm miễn phí. Ngoài việc làm phiền, adware có thể làm giảm đáng kể hiệu suất của máy tính, làm chậm, treo máy.

Spyware là một phần mềm thực hiện đánh cắp thông tin từ máy tính mà người dùng không hề hay biết. Phần mềm miễn phí thường có rất nhiều spyware, vì vậy

trước khi cài đặt cần đọc kĩ thỏa thuận sử dụng. Một trường hợp đáng chú ý nhất về spyware liên quan tới vụ tai tiếng chống copy đĩa CD BMG của Sony.

Đa số những chương trình chống spyware tốt sẽ nhanh chóng tìm ra và gỡ bỏ adware/spyware khỏi máy tính. Bạn cũng nên thường xuyên xóa những file tạm, cookies và history từ các trình duyệt Web để phòng nhừa nhóm malware này.

Malware stew

Cho đến nay, tất cả các loại malware được biết đến đều khá khác nhau, giúp có thể phân biệt từng loại. Tuy nhiên, loại malware stew này không giống như vậy. Những người viết nó đã nghiên cứu làm thể nào để kết hợp những đặc tính tốt nhất của nhiều loại malware khác nhau để nâng cao khả năng của nó.

Rootkit là một ví dụ điển hình của loại malware này, nó gồm các đặc tính của một Trojan horse và một Backdoor. Khi được sử dụng kết hợp, tin tặc có thể giành quyền kiểm soát máy tính từ xa mà không bị nghi ngờ.

Rootkits

Rootkit là loại hoàn toàn khác biệt, chúng thường sửa đổi hệ điều hành hiện thời thay vì bổ sung những phần mềm ở mức ứng dụng mà những loại malware khác thường làm. Điều này rất nguy hiểm bởi vì những chương trình chống malware sẽ rất khó phát hiện được chúng.

Có nhiều loại rootkits, trong đó có 3 loại được cho là nguy hiểm nhất, gồm: user-mode, kernel mode và firmware rootkits.

User-mode rootkits

User-mode gồm những đoạn mã giới hạn truy cập vào tài nguyên phần mềm và phần cứng trên máy tính. Hầu hết những mã chạy trên máy tính sẽ chạy trên chế độ user-mode. Vì truy cập bị giới hạn nên những phá hủy trong user-mode là không thể phục hồi.

User-mode rootkit chạy trên máy tính với quyền admin. Điều đó có nghĩa:

- User-mode rootkits có thể thay đổi tiến trình, file, ổ hệ thống, cổng mạng và thậm chí là dịch vụ hệ thống.

- User-mode rootkit tự duy trì cài đặt bằng cách sao chép những file yêu cầu vào ổ cứng máy tính và tự động khởi chạy mỗi khi hệ thống khởi động.

Hacker Defender là một user-mode rootkit điển hình. Loại rootkit này và nhiều loại khác bị phát hiện và gở bỏ bởi ứng dụng nổi tiếng của Luckily Mark Russinovich.

Kernel-mode rootkits

Kernel-mode gồm những mã hủy giới hạn truy cập vào mọi tài nguyên phần cứng và phần mềm trên máy tính. Kernel-mode thường được dùng để lưu trữ những chức năng tin cậy nhất của hệ điều hành. Những hủy hoại trong kernel-modecũng không thể phục hồi.

Từ khi rootkit chạy trong chế độ user-mode bị phát hiện và gỡ bỏ, những người lập trình rootkit đã thay đổi tư duy và phát triển kernel-mode rootkit. Kernel-mode có nghĩa là rootkit được cài đặt đồng mức với hệ thống và những chương trình phát hiện rootkit. Vì vậy rootkit có thể làm cho hệ thống không còn đáng tin cậy nữa.

Không ổn định là một dấu hiệu sa sút của hệ thống một kenel-mode rootkit gây ra, thậm chí dẫn đến những hủy hoại không rõ nguyên nhân hay treo màn hình. Lúc đó, bạn nên thử GMER, một trong số ít công cụ gỡ bỏ rootkit có thể tin cậy, để chống lại kernel-mode rootkit như Rustock.

Firmware rootkits

Firmware rootkit là loại rootkit cài đặt tinh vi vì những người phát triển loại rootkit này đã nghiên cứu phương pháp lưa trữ malcode của rootkit trong firmware. Mọi firmware đều có thể bị thay đổi, từ mã vi xử lý cho tới firmware của khe cắm mở rộng. Điều đó có nghĩa:

- Khi tắt máy, rootkit ghi malcode hiện thời vào những firmware khác nhau.
- Khi khởi động lai máy tính rootkit cũng tự thực hiện cài đặt lại.

Thậm chí, nếu một chương trình phát hiện và gỡ bỏ được firmware rootkit, thì lần khởi động máy tính sau, firmware rootkit này vẫn xuất hiện hoạt động trở lại bình thường.

6. Malicious mobile code (Mã độc di động – MMC)

MMC nhanh chóng trở thành phương pháp cài đặt malware vào máy tính hiệu quả nhất. Chúng có thể:

- Chiếm quyền máy chủ từ xa.
- Di chuyển trong mạng.
- Tải và cài đặt trên một hệ thống cục bộ

MMC gồm Javascript, VBScript, ActiveX Controls và Flash Animations. Mục đích chính rất dễ nhận ra của MMC là cách thức hoạt động, nó làm nội dung trang của trình duyệt web trở nên tương tác hơn.

Tại sao MMC lại độc hại? Vì việc cài đặt nó không cần đến sự cho phép của người dùng và gây hiểu lầm cho người dùng. Ngoài ra nó thường là bước đệm cho một cuộc tấn công kết hợp giống như công cụ xâm nhập mà Trojan horse malware sử dụng. Sau đó tin tặc có thể tiến hành cài đặt thêm nhiều malware.

Cách tốt nhất để chống lại MMC là luôn cập nhật hệ thống và tất cả chương trình phụ.

7. Blended threat (Mối đe dọa hỗn hợp)

Malware được cho là một blended threat khi nó gây ra những tổn hại lớn và phát tán nhanh chóng thông qua những phần kết hợp của nhiều malcode có mục tiêu riêng. Blended threat xứng đáng là mối lo ngại đặc biệt vì nhiều chuyên gia bảo mật cho rằng chúng là "những chuyên gia trong công việc của chúng". Một blended threat điển hình có thể:

- Khai thác và tạo ra nhiều lỗ hổng.
- Sử dụng nhiều phương thức tái tạo khác nhau.
- Tự động chạy mã hủy can thiệp của người dùng.

Ngoài ra, blended threat malware có thể gửi một email dạng HTML nhúng Trojan horse cùng với một file PDF đính kèm chứa một loại Trojan horse khác. Một số loại blended threat khá quen thuộc là Nimda, CodeRed và Bugbear. Để gỡ bỏ blended threat khỏi máy tính cần đến nhiều chương trình chống malware, cũng như sử dụng chương trình quét malware được cài đặt chạy trực tiếp từ đĩa CD.

8. Bots

Robot được tự động thực thi hay bots khá phổ biến trong Internet hiện đại. Chúng thường được sử dụng để tự động hóa các tác vụ nhàm chán, lặp đi lặp lại, hay gặp nhất là trong những cuộc đấu giá trực tuyến, kiểm tra trực tuyến, chat và chơi game.

Tuy nhiên, có một mặt tối khác là bots bị sử dụng cho những mục đích xấu như gửi thư spam, phát tán phần mềm độc hại khác cũng như tham gia vào mạng lưới botnet: một mạng máy tính khổng lồ, đã bị nhiễm malware và dùng để thực hiện những vụ tấn công mạng quy mô lớn.

Phần mềm diệt virus có thể bảo vệ máy tính khỏi những malware dạng bots này nhưng có vài trường hợp mà rootkit được cài đặt trước, ngăn chặn phần mềm diệt virus phát hiện bots, nên việc quét rootkit thường xuyên là biện pháp phòng ngừa tốt nhất.

9. Ransomware

Ransomware là một trong những công cụ kiếm tiền lớn nhất của hacker. Về bản chất, nó mã hóa dữ liệu trên máy tính, yêu cầu một khoản tiền chuộc để mở khóa dữ liệu. Một số ransomware "lởm" thì chỉ khóa máy tính (cho phép gỡ bỏ dễ dàng trong chế độ Safe Mode), trong khi những loại nguy hiểm hơn sẽ mã hóa toàn bộ ổ cứng, chặn quyền truy cập của người dùng cho đến khi kẻ tấn công nhận được tiền (thường dưới dạng Bitcoin hoặc thông qua chuyển khoản ẩn danh như Western Union).

Hacker thường đe dọa người dùng rằng chúng tìm thấy những tài liệu phạm pháp hoặc đáng ngờ trên ổ cứng. Để có thêm bằng chứng, hacker có thể sử dụng webcam chụp hình nạn nhân. Chiến thuật này của hacker có thể gây hoảng loạn, khiến nạn nhân phải bỏ tiền chuộc vì sợ hãi và tuyệt vọng.

Ransomware lây nhiễm vào một máy tính theo cách thức khá giống với Trojan horse, thông qua tải file về và chạy file. Cách khác để ransomware lây nhiễm vào mạng máy tính là thông qua một lỗ hổng của mạng hay rootkit. Nói chung, một chương trình chống virus được cập nhật có thể phát hiện malware dạng này trước khi chúng kịp tác quái.

Trong tương lai, với sự phát triển và thâm nhập ngày càng sâu rộng của Internet vào cuộc sống thì số lượng, dạng malware sẽ ngày càng gia tăng. Dù các nhà phát hành ứng dụng, hệ điều hành cũng thường xuyên phát hành các bản vá lỗ hổng, đưa thêm công cụ để ngăn chặn malware nhưng chừng đó là chưa đủ. Chúng ta cần thường xuyên cập nhật những phiên bản phần mềm, hệ điều hành mới, luyện tập thói quen cẩn thận khi nhấp chuột, tải file, lướt net để giảm thiểu nguy cơ nhiễm malware.